MASTER OF SCIENCE IN CYBERSECURITY

Dr. Afzal Upal, Academic Director
Master of Science in Cybersecurity
Address: University of Wisconsin-Platteville
1 University Plaza
Platteville, WI 53818-3099
Phone: 608.342.1625
Email: upala@uwplatt.edu

STATEMENT OF PURPOSE

This program represents a comprehensive, multidisciplinary curriculum that prepares students to advance their careers and pursue their academic ambitions through leadership and management positions within the cybersecurity field. The program will equip students with the skills needed to effectively develop, implement, and maintain a security strategy within diverse organizations and industry sectors.

STUDENT LEARNING OUTCOMES

Graduates will:

- Analyze and resolve security issues in networks and computer systems to secure an IT infrastructure
- Design, develop, test, and evaluate secure software
- Develop policies and procedures to manage enterprise security risks
- Evaluate and communicate the human role in security systems with an emphasis on ethics, social engineering vulnerabilities, and training
- Interpret and forensically investigate security incidents

INTRODUCTION

This program represents a comprehensive, multidisciplinary curriculum that prepares students to advance their careers and pursue their academic ambitions through leadership and management positions within the cybersecurity field. The program will equip students with the skills needed to effectively develop, implement, and maintain a security strategy within diverse organizations and industry sectors. Core courses provide students with a solid foundation in data and network security, compliance, strategic planning, program design and management, legal and ethical issues in cybersecurity, cryptography, risk management, and technical communications. In addition, the program offers four unique tracks to assist students in tailoring their coursework to meet their career goals: digital forensics, cyber response, governance and leadership, and security architecture. The Master of Science in Cybersecurity represents a fully online, asynchronous curriculum comprised of 34 credits to include a culminating, project-based capstone experience. Graduates of the program will gain the core competencies required to assume a variety of roles across a wide range of industries to include cybersecurity analyst, security consultant, cybersecurity manager, computer system analyst, security application analyst, and information technology specialist.

ADMISSION REQUIREMENTS FOR MASTER OF SCIENCE IN CYBERSECURITY

Admission to the Master of Science in Cybersecurity requires:

- Prerequisite coursework in Introduction to Computer Science (with a programming emphasis) and Calculus or Statistics
- A bachelor’s degree from an accredited university
- Employment résumé
- Two letters of recommendation
- A personal statement of not more than 1000 words
- Admission exams, such as the GRE or the GMAT, are not required.

To be eligible for admission in full standing, a student must have an overall undergraduate grade point average of 2.5. Students who do not qualify for admission in full standing may be admitted on a trial enrollment justified by the admitting department and approved by the dean of the School of Graduate Studies. Students are allowed seven years from the date of admission into the program to complete degree requirements; extensions may be granted for extenuating circumstances.

Program entrance requirements and degree completion requirements are consistent with those of the other collaborative degree-granting institutions offering this program. Applicants should follow the instructions found in the Online Admission Policies and Procedures section of this catalog.

SPECIAL STUDENTS

Students who have earned a bachelor’s degree from a nationally or regionally accredited institution recognized by the Council for Higher Education Accreditation may register as a Special Student. Students will receive academic credit for courses taken while on this status. Students can be considered for admission into a degree program if they maintain a 3.00 grade point average in all graduate-level work and all other admission requirements are met. With the program area advisor’s approval, students may transfer up to 12 credits earned at UW-Platteville into a degree program. All graduate-level work will be included in computing a student’s GPA.

CURRICULUM

The Cybersecurity degree program has a 34-credit curriculum, wherein students will complete a 25 core credits (including a 3-credit Capstone course) and 9 credits of electives from one of four emphasis to satisfy degree requirements.

Course	Title	Credits
Core courses		
CYB 7000	Cybersecurity Fundamentals	3
CYB 7030	Network Security	3
CYB 7050	Cybersecurity and Society	3
CYB 7070	Cybersecurity Planning	3
CYB 7100	Introductory Cryptography	3
CYB 7150	Managing Security Risk	3
CYB 7200	Technical Communication	3
CYB 7890	Pre Capstone	1
CYB 7900	Capstone	3

CYBER RESPONSE EMPHASIS

The Cyber Response emphasis area consists of the following three courses

Course	Title	Credits
CYB 7400	Incident Response	3
CYB 7450	Secure Operating Systems	3
CYB 7500	Offensive Security & Threat Management	3
Total Credits		9

DIGITAL FORENSICS EMPHASIS

The Digital Forensics emphasis area consists of the following three courses

Course	Title	Credits
CYB 7250	Computer Forensics	3
CYB 7300	Computer Criminology	3
CYB 7350	Network Forensics	3
Total Credits		9

GOVERNANCE AND LEADERSHIP EMPHASIS

The Governance and Leadership area consists of the following three courses

Course	Title	Credits
CYB 7550	Security Administration	3
CYB 7600	Leadership & Teams	3
CYB 7650	Cybersecurity Management	3
Total Credits		9

SECURITY ARCHITECTURE EMPHASIS

The **Security Architecture** emphasis area consists of the three of the following four courses

Course	Title	Credits
CYB 7700	Security Architecture	3
CYB 7800	Software Security	3
CYB 7850	Cyber-Physical System Security	3

or CYB 7750	Applied Cryptography	
Total Credits		9